Specification

Title of the Invention

[0001] Wireless Communication System
Exchanging Encrypted Data

Background of the Invention

[0002] The present invention relates to a wireless communication system having a plurality of electronic devices that exchange encrypted data with a wireless transmission.

[0003] Conventionally, wireless communication systems typically known as a wireless LAN (Local Area Network) are in widespread use. In the wireless communication system, in order to keep secrecy of data exchanged between the electronic devices, encryption system is generally employed.

[0004] In a transmitting station, data is encrypted before transmitted using a predetermined data (which will be referred to as ciphering data) for encryption. In a receiving station which receives the thus encrypted data, the encrypted data is decoded using deciphering data. It should be noted that, when the ciphering data used for encrypting and the deciphering data used for decoding are the same, i.e., the ciphering data used for encrypting can also be used for decoding, the deciphering

data is also called as the ciphering data.

[0005] As the encryption system, a public key encryption system in which the ciphering data and the deciphering data are different, and a common key encryption system in which the ciphering data and the deciphering data are the same have generally been known. It is also known that the common key encryption system requires less processing load to the communication system than the public key encryption system since the same ciphering/deciphering data is used in the transmitting and receiving stations.

[0006] In the encrypting/decoding system that does not require that the deciphering data is transmitted from the receiving station to the transmitting station, there is little chance that the deciphering data is known by other stations. Thus, in such a system, the encrypted data will hardly be decoded by other stations, and the secrecy of the data can be kept.

[0007] An example of the communication system employing the public key encrypting system is disclosed in Japanese Patent Application Provisional Publication No. HEI 10-224340. According to the system disclosed in this publication, in order to improve the secrecy of data exchanged between a wireless transmitting station and a wireless receiving station, data such as a pop table is encrypted using public key data (i.e., the ciphering data), and the encrypted data is transmitted to the receiving station. Then, in the receiving station, with use

of preliminary set secret key data (i.e., deciphering data), the received data is decoded. In this system, data should be encrypted using the public key data that corresponds to the secret key data, and thus, the public key data has been transmitted from the receiving station to the transmitting station.

[0008] In the common key encrypting system, the same key data (i.e., the common key data) is used for encrypting in the transmitting station, and for decoding in the receiving station. If, in such a system, the common key data is transmitted from the receiving station to the transmitting station, it may be received by another station which is not intended by a user. It should be noted that, any station which receives the common key data, can decode the encrypted data using the same common key data, and it is hard to keep the secrecy in such a case.

Summary of the Invention

[0009] The present invention is advantageous in that, in an environment where the deciphering data is to be transmitted/received between the transmitting station and the receiving station, secrecy of the encrypted data exchanged therebetween by a wireless communication can be kept.

[0010] According to an aspect of the invention, there is provided a wireless communication system including a terminal

device that transmits a wireless signal and an electronic device that receives the wireless signal transmitted by the terminal device. In particular, the terminal device is provided with an encrypting system that encrypts data to be transmitted, a first communication system that transmits deciphering data to the electronic device with a wireless signal having a directivity, and a second communication system that transmits the encrypted data to the electronic device with a wireless signal which does not have the directivity. Further, the electronic device is provided with a third communication system that receives the wireless signal transmitted by the transmitting system of the terminal device, and a decoding system that decodes the encrypted data that is received through the third communication system using the deciphering data that is received through the third communication system.

[0011] According to another aspect of the invention, there is provided a wireless communication system including a terminal device that transmits a wireless signal and an electronic device that receives the wireless signal transmitted by the terminal device. In such a communication system, the electronic device may be provided with a first communication system that transmits ciphering data to be used for encrypting data to the terminal device with a wireless signal having a directivity, a second communication system that receives encrypted data to be processed, the second communication system

does not have directivity, and a decoding system that decodes the encrypted data received through the second communication system using the deciphering data corresponding to the ciphering data transmitted by the first communication system. Further, the terminal device may be provided with a third communication system that is capable of receiving the ciphering data transmitted by the first communication system and transmitting data to the second communication system, and an encrypting system that encrypts data to be processed using the ciphering data received through the third communication system, the encrypted data being transmitted to the second communication system through the third communication system.

[0012] Optionally, in each of the above configurations, the first communication system may be provided with a directional antenna, and the second communication system may be provided with an omnidirectional antenna.

[0013] Further optionally, a communication between the first communication system and the third communication system and a communication between the second communication system and the third communication system may be performed in accordance with the same communication protocol.

[0014] In a particular case, the ciphering data is identical to the deciphering data. Alternatively, the ciphering data and the deciphering data may be different from each other.

[0015] Still optionally, the third communication system

may not have the directivity.

[0016] Further optionally, the first communication system may be provided with a directional antenna, and the second communication system may be provided with an omnidirectional antenna.

[0017] According to another aspect of the invention, there is provided a terminal device for a wireless communication system including the terminal device and an electronic device. The terminal device may be provided with an encrypting system that encrypts data to be transmitted to the electronic device, a first communication system that transmits deciphering data to the electronic device with a wireless signal having a directivity, and a second communication system that transmits the encrypted data to the electronic device with a wireless signal which does not have the directivity, the encrypted data being decodable using the deciphering data transmitted by the first communication system.

[0018] Optionally, the first communication system may be provided with a directional antenna, and the second communication system may be provided with an omnidirectional antenna.

[0019] Further, the ciphering data may be identical to the deciphering data. Alternatively, they could be different from each other.

[0020] According to a further aspect of the invention,

there is provided an electronic device for a wireless communication system including a terminal device and the electronic device. Specifically, the electronic device may include a first communication system that transmits ciphering data to be used for encrypting data to the terminal device with a wireless signal having a directivity, a second communication system that receives data to be processed from the terminal device, the second communication system does not have directivity, the data transmitted from the terminal device being encrypted using the ciphering data transmitted by the first communication system, and a decoding system that decodes the encrypted data received through the second communication system using the deciphering data corresponding to the ciphering data transmitted by the first communication system.

[0021] Optionally, the first communication system may be provided with a directional antenna, and the second communication system may be provided with an omnidirectional antenna.

[0022] Further, the ciphering data may be identical to the deciphering data. Alternatively, they could be different from each other.

[0023] According to a furthermore aspect of the invention, there is provided device implemented with a program that enables the device to function as a terminal device for a wireless communication system including the terminal device and an

electronic device. The terminal device realized by the program may include an encrypting system that encrypts data to be transmitted to the electronic device, a first communication system that transmits deciphering data to the electronic device with a wireless signal having a directivity, and a second communication system that transmits the encrypted data to the electronic device with a wireless signal which does not have the directivity, the encrypted data being decodable using the deciphering data transmitted by the first communication system.

[0024] According to another aspect of the invention, there is provided a device implemented with a program that enables the device to function as an electronic device for a wireless communication system including a terminal device and the electronic device. The electronic device realized by the program may include a first communication system that transmits ciphering data to be used for encrypting data to the terminal device with a wireless signal having a directivity, a second communication system that receives data to be processed from the terminal device, the second communication system does not have directivity, the data transmitted from the terminal device being encrypted using the ciphering data transmitted by the first communication system, and a decoding system that decodes the encrypted data received through the second communication system using the deciphering data corresponding to the ciphering data transmitted by the first communication system.

[0025] It should be noted that the systems and devices according to the present invention can be realized when appropriate programs provided and executed by a personal computer or the like. Such programs may be stored in recording medium such as a flexible disk, CD-ROM, memory cards and the like and distributed. Alternatively or optionally, such programs can be distributed through networks such as the Internet.

Brief Description of the Accompanying Drawings

[0026] Fig. 1 is a block diagram of a printer and a personal computer of a wireless communication system according to a first embodiment of the invention;

[0027] Fig. 2 schematically shows an appearance of the printer shown in Fig. 1;

[0028] Fig. 3 schematically shows an appearance of the personal computer shown in Fig. 1;

[0029] Fig. 4 is a flowchart illustrating a transmission procedure executed by a CPU of the personal computer;

[0030] Fig. 5 is a flowchart illustrating a normal data communication executed in the transmission procedure shown in Fig. 4;

[0031] Fig. 6 is a block diagram of a printer and a personal computer of a wireless communication system according to a

second embodiment of the invention;

[0032] Fig. 7 schematically shows an appearance of the printer shown in Fig. 6;

[0033] Fig. 8 schematically shows an appearance of the personal computer shown in Fig. 6;

[0034] Fig. 9 is a flowchart illustrating a transmission procedure executed by a CPU of the printer; and

[0035] Fig. 10 is a flowchart illustrating a normal data communication executed in the transmission procedure shown in Fig. 9.

Detailed Description of the Embodiments

[0036] Hereinafter, referring to the accompanying drawings, wireless communication systems according to embodiments of the invention will be described.

[0037] First Embodiment

[0038] Fig. 1 is a block diagram of a printer 101 and a personal computer (PC) 121 of a wireless communication system 100 according to a first embodiment of the invention. In the embodiment, the printer 101 serves as an example of an electronic device, and the personal computer 121 serves as an example of a terminal device. In Fig. 1, for the brevity, only one printer 101 and one personal computer 121 are shown. It

should be noted that the communication system 100 could be configured to have a plurality of printers, personal computers, and other electronic devices and terminal devices.

[0039] As shown in Fig. 1, the printer 101 has a CPU (Central Processing Unit) 102, a ROM (Read Only Memory) 103, a RAM (Random Access Memory) 104, a printing unit 105, a display unit 106, an operation unit 107, an RF (Radio Frequency) module 108 and an omnidirectional antenna 113.

[0040] The CPU 102, the ROM 103, the RAM 104, the printing unit 105, the display unit 106, the operation unit 107 and the RF module 108 are interconnected through a system bus 110. The omnidirectional antenna 113 is connected to the RF module 108.

[0041] The CPU 102 controls the entire operation of the printer 101. In particular, the CPU 102 controls the printing unit 105 to provide the printer function. The CPU 102 also analyzes data received and executes a deciphering program 103a (described later) to decode encrypted data.

[0042] The ROM 103 is a read only memory and serves as a part of a main memory space to be used by the CPU 102. The ROM 103 stores the deciphering program 103a. The deciphering program 103a is for decoding the encrypted data using deciphering data stored in a deciphering data table 104a which is stored in the RAM 104.

[0043] The RAM 104 is a readable/writable memory, which also serves as a part of the main memory space used by the CPU

102. As mentioned above, the RAM 104 stores the deciphering data table 104a. The deciphering data table 104a stores the deciphering data (in the present embodiment, the common key encrypting system is employed, and accordingly, the deciphering data is identical to the ciphering data which is used either for the ciphering and deciphering). It should be noted that the ciphering data (deciphering data) transmitted to the PC 121 is stored (added) to the deciphering data table 104a in relationship with the PC 121 which transmitted the data. It should be noted that data processing speed when the common key encrypting system is employed is faster than a case where the public key system is employed.

[0044] The printing unit 105 provides a printing function for printing monochromatic or color characters/images. The printing unit 105 is connected to the system bus 110 through an I/O (input/output) interface (not shown). The printing unit 105 is used, under control of the CPU 102, for printing out the print data transmitted, for example, from the PC 121.

[0045] The display unit 106 is for displaying various information using a display device. The display unit 106 is connected to the system bus 110 through an I/O interface (not shown). The display unit 106 is used, under control of the CPU 102, for displaying information related to functions of the printer 101. The display unit 106 typically includes an LCD (Liquid Crystal Display) panel.

[0046] The operation unit 107 is an input device provided to the printer 101 for allowing a user to input various commands/data. The operation unit 107 is also connected to the system bus 110 through an I/O interface (not shown). The operation unit 107 includes a power switch and function buttons related to available functions thereof. The operation unit 107 typically includes a key array provided with a plurality of operation keys.

[0047] The RF module 108 is a module used for the wireless communication. Typically, the RF module 108 is a digital circuit including a transmitter and a receiver. The RF module 108 is connected to the system bus 110 through a not shown I/O interface. The RF module 108 is connected with the omnidirectional antenna 113.

[0048] The omnidirectional antenna 113 transmits a radio wave in non-specified direction (i.e., the omnidirectional antenna 113 is not designed for a directional wireless communication). As described above, the omnidirectional antenna 113 is connected with the RF module 108. As examples of the omnidirectional antenna 113, a diversity antenna and a whip antenna are well known.

[0049] As shown in Fig. 1, the PC 121 includes a CPU 122, a ROM 123, a RAM 124, an HDD (Hard Disk Driver) 125, a display unit 126, an operation unit 127, an RF module 128, an antenna switching unit 129, a directional antenna 131 and an

omnidirectional antenna 132. The CPU 122, the ROM 123, the RAM 124, the HDD 125, the display unit 126, the operation unit 127, the RF module 128 are interconnected through a system bus 130. The directional antenna 131 and the omnidirectional antenna 132 are connected to the RF module 128 through the antenna switching unit 129.

[0050] The CPU 122 controls entire operation of the PC 121. The CPU 122 selectively retrieves programs (e.g., an encrypting program for encrypting data to be transmitted, and a program for transmitting the encrypted print data to an electronic device) from the HDD 125.

[0051] The ROM 123 is a read only memory, and serves as a part of the main memory space for the CPU 122. A boot program for starting up an operating system of the PC 121 is also stored in the ROM 123. The RAM 124 is a readable/writable memory, and serves as a part of the main memory space for the CPU 122.

[0052] The HDD 125 includes a readable/writable medium (i.e., a hard disk) and a device for reading/writing data on the hard disk. In the HDD 125, an encrypting program 125a, a ciphering data table 125b, a program for transmitting the encrypted data, and the data to be transmitted to the printer 101 are stored.

[0053] The encrypting program 125a encrypts data using the ciphering data stored in the ciphering data table 125b. It should be noted that the ciphering data is generated every time

when a cipher code exchanging protocol is executed and is stored/added in the ciphering data table 125b.

[0054] The display unit 126 is for displaying various information on a display device. The display unit 126 is connected to the system bus 130 through a not shown I/O interface. The display unit 126 is used, under control of the CPU 122, for displaying various information related to functions of the PC 121. The display unit 126 typically includes an LCD panel.

[0055] The operation unit 127 is an input device provided to the PC 121 for allowing the user to input various commands/data. The operation unit 127 is also connected to the system bus 130 through a not shown I/O interface. The operation unit 127 typically includes a mouse and a keyboard provided with a plurality of keys.

[0056] The RF module 128 is a module used for the wireless communication. Typically, the RF module 128 is a digital circuit including a transmitter and a receiver. The RF module 128 is connected to the system bus 130 through a not shown I/O interface. The RF module 128 is connected with the directional antenna 131 and the omnidirectional antenna 132 through the antenna switching unit 129.

[0057] It is preferable that the directional antenna 131 and the omnidirectional antenna 132 are for the same frequency band, and use a common circuit (i.e., the RF module 108).

[0058] The antenna switching unit 129 is for switching the

antenna to be connected to the RF module 128. That is, the antenna switching unit 129 is connected with the directional antenna 131 and the omnidirectional antenna 132, one of which is selectively connected to the RF module 128.

[0059] The directional antenna 131 is capable of transmitting/receiving radio wave to/from a specific direction (i.e., the directional antenna 131 is designed to perform a directional wireless communication). As examples of the directional antenna, a Yagi antenna and a parabolic antenna have been well known.

[0060] The omnidirectional antenna 132 transmits a radio wave in non-specified direction (i.e., the omnidirectional antenna 132 is not designed for a directional wireless communication). As examples of the omnidirectional antenna 132, a diversity antenna and a whip antenna are well known.

[0061] Next, an electronic device 1 (e.g., the printer 101) and a terminal device 2 (e.g., the PC 121) according to the first embodiment will be described in detail.

[0062] Fig. 2 schematically shows an appearance of the electronic device 1 (e.g., the printer), and Fig. 3 schematically shows an appearance of the terminal device 2 (e.g., the PC). It should be noted that, the electronic device 1 needs not be limited to the printer 101, and other apparatus or equipment, which stores, prints and/or transmits image data and/or document data having secrecy, such as a multifunction

peripheral having functions of a facsimile device and the printer, a facsimile machine, a scanner, a device having functions of a file server or a file storage, a stream server, a wireless LAN access point, a Bluetooth access point, may be used as the electronic device 1.

[0063] The electronic device 1 is provided with an omnidirectional antenna 1c (e.g., the omnidirectional antenna 113 shown in Fig. 1) and a table 1d. As the omnidirectional antenna 1c, a diversity antenna or a whip antenna can be used. The omnidirectional antenna 1c may be formed integrally with a body of the electronic device 1c, or a card type one such as a wireless LAN card having a built-in antenna. The table 1d is provided to the body of the electronic device 1 so as to be opened/closed with respect to the body. When the table 1d is opened as show in Fig. 2, the terminal device 2 can be placed thereon. Preferably, when the terminal device 2 is placed on the table 1d, a receiving direction of the omnidirectional antenna 1c and a transmission direction of a directional antenna 2a meet each other. It should be noted that the table 1d needs not be provided to the electronic device 1.

[0064] The terminal device 2 needs not be limited to the PC 121, and any other apparatus that makes use of other electronic device for obtaining, storing, printing and/or transmitting image data and/or document data having secrecy, such as a PDA (Personal Digital Assistant), a cellular phone,

a portable game machine, a wireless digital camera, and a wireless video camera can be used as the terminal device 2. The terminal device 2 includes a directional antenna 2a and an omnidirectional antenna 2b. As the directional antenna 2a, the Yagi antenna and the parabolic antenna can be used. As the omnidirectional antenna 2b, the diversity antenna and the whip antenna can be used. It should be noted that the directional antenna 2a may be one, as shown in Fig. 3, integrally formed on the body of the terminal device, or a card type device having a built-in antenna. Similarly, the omnidirectional antenna 2b may be a card type device having the built-in antenna as shown in Fig. 3 or one integrally formed to the body of the terminal device 2.

[0065] Next, a procedure, executed in the terminal device 2, for transmitting the encrypted data to the electronic device 1 will be described with reference to Figs. 4 and 5.

[0066] Fig. 4 is a flowchart illustrating a transmission procedure executed by a CPU of the PC 121, and Fig. 5 is a flowchart illustrating a normal data communication called in the transmission procedure shown in Fig. 4.

[0067] As shown in Fig. 4, the CPU 122 of the PC 121 (i.e., the terminal device) controls the antenna switching unit 129 to connect the omnidirectional antenna 132 to the RF module 128, and disconnect the directional antenna 131 from the RF module 128 (S101).

[0068] Then, the PC 121 executes a normal data communication (S102), which will be described later, with respect to the printer 101 (i.e., the electronic device). In S103, the CPU 122 determines whether the data transmission is successfully finished. It should be noted that whether the data transmission has been successfully done is determined taking the execution of the ciphering data exchange protocol into account. That is, when the ciphering data exchange protocol has been executed, the transmission of the data is determined to be successful. However, if the ciphering data exchange protocol has not bee executed, the data transmission is determined to be failed.

[0069] When the data transmission is determined to be finished successfully (S103: YES), control returns to S101. When the data transmission is determined to be failed (S103: NO), it is further determined whether a ciphering data exchange request has been transmitted from the printer 101 (S104).

[0070] When the printer 101 has not issued the ciphering data exchange request (S104: NO), an error message indicating that the connection with the printer 101 cannot be established is displayed (S108), and control returns to S101.

[0071] When it is determined that the printer 101 has issued the ciphering data exchange request (S104: YES), the CPU 122 controls the antenna switching unit 129 to connect the omnidirectional antenna 132 to the RF module 128, and disconnect

the directional antenna 131 from the RF module (S105).

[0072] Next, between the omnidirectional antenna 113 of the printer 101 and the directional antenna 131 of the PC 121, the exchanging protocol of the ciphering data of the common key encrypting system (note that the ciphering data is identical to the deciphering data) is executed (S106).

[0073] Then, the ciphering data, which was generated as the exchanging protocol was executed and transmitted to the printer 101, is registered with the ciphering data table 125b stored in the HDD 125 in relationship with the printer 101 in S107. In the printer 101, the ciphering data received from the PC 121 is registered with the deciphering data table 104a in relationship with the PC 121.

[0074] With the above procedure, the exchange of the ciphering data is finished. Thereafter, the CPU 122 controls the antenna switching unit 129 to connect the omnidirectional antenna 132 with the RF module 128 and disconnect the directional antenna 131 from the RF module 128 (S108). Then, control returns to S101.

[0075] Next, the normal data communication, which is called in S102 of Fig. 4, will be described with reference to Fig. 5.

[0076] Firstly, the CPU 122 determines whether the ciphering data corresponding to the printer 101 is stored in the ciphering data table 125b (S10201). When the ciphering data

corresponding to the printer 101 is not stored in the ciphering data table 125b (S10201: NO), the normal data communication is terminated. When the ciphering data corresponding to the printer 101 is stored in the ciphering data table 125b (S10201: YES), the CPU 122 encrypts the data to be transmitted using the encrypting program 125a, referring to the ciphering data corresponding to the printer 101, which has been registered with the ciphering data table 125b (S10202). The, the thus encrypted data is transmitted to the printer 101 (S10203).

[0077] In the printer 101, when the data encrypted using the ciphering data is received from the PC 121, the received encrypted data is decoded using the deciphering program 103a with reference to the ciphering data which was exchanged in S106 and registered with the ciphering data table 104a.

[0078] It should be noted that the communication between the omnidirectional antenna 113 and the directional antenna 131, and the communication between the omnidirectional antenna 113 and the omnidirectional antenna 132 are executed using the same communication protocol. When the same communication protocol is used, only communication paths are different, and the wireless signal processing operations are identical. Therefore, the processing of the wireless signals becomes identical, which is convenient and will not increase load to the system.

[0079] As above, with the communication system 100 according to the first embodiment, the ciphering data to be

referred to for deciphering, which is stored in the ciphering data table 125b of the PC 121, is transmitted through the directional antenna 131 (S105-S106).

[0080] As a result, the printer 101 which can receive the ciphering data is limited, and a possibility of tapping of the ciphering data is lowered, and accordingly, the secrecy of the transmitted data can be kept.

[0081] Further, according to the first embodiment, the encrypted data using the ciphering data is transmitted from the PC 121 using the omnidirectional antenna 132 (S101 and S102). As a result, the direction of the encrypted data transmitted from the PC 121 needs not be precisely adjusted to meet the printer 101, which is convenient and reduces communication errors.

[0082] As described above, a directional mode transmission of the wireless signal can be realized using a generally used directional antenna 131 (e.g., the Yagi antenna), and the omnidirectional mode transmission of the wireless signal is realized using the generally used omnidirectional antenna 132 (e.g., the diversity antenna).

[0083] According to the communication system described above, only by configuring the PC 121 to perform the directional mode transmission of the wireless signal and the omnidirectional mode transmission of the wireless signal, the secrecy is improved. No extra structures for improving the

secrecy need not be provided to the PC 121 or the printer 101. Thus, the secrecy of the entire system can be improved relatively simply.

[0084] Second Embodiment

[0085] Next, a communication system according to a second embodiment will be described with reference to Fig. 6.

[0086] Fig. 6 is a block diagram of a printer 201 and a personal computer (PC) 221 of a wireless communication system 200 according to the second embodiment of the invention. In the second embodiment, the printer 201 serves as an example of an electronic device, and the PC 221 serves as an example of a terminal device. In Fig. 6, for the brevity, only one printer 201 and one PC 221 of the communication system 200 are shown. It should be noted that the communication system 200 could be configured to have a plurality of printers, personal computers, and other electronic devices and/or terminal devices.

[0087] As shown in Fig. 6, the printer 201 has a CPU 202, a ROM 203, a RAM 204, a printing unit 205, a display unit 206, an operation unit 207, an RF module 208, an antenna switching unit 209, a directional antenna 211, an omnidirectional antenna 212 and a timer 213. The CPU 202, the ROM 203, the RAM 204, the printing unit 205, the display unit 206, the operation unit 207, the RF module 208 and the timer 213 are interconnected through a system bus 210. The directional antenna 211 and the

omnidirectional antenna 212 are connected to the RF module 208 through the antenna switching unit 209.

[0088] The CPU 202 controls the entire operation of the printer 201. In particular, the CPU 202 controls the printing unit 205 to provide the printer function. The CPU 202 also analyzes data received and executes a deciphering program 203a (described later) to decode encrypted data. The CPU 202 further retrieves program for receiving the encrypted data from the terminal device (i.e., PC 221).

[0089] The ROM 203 is a read only memory and serves as a part of a main memory space to be used by the CPU 202. The ROM 203 stores the deciphering program 203a, and another program for receiving the encrypted data from the terminal device (e.g., the PC 221). The deciphering program 203a is for decoding the encrypted data using deciphering data registered in a deciphering data table 204a stored in the RAM 204.

[0090] The RAM 204 is a readable/writable memory, which also serves as a part of the main memory space used by the CPU 202. The RAM 204 stores the deciphering data table 204a. The deciphering data table 204a stores deciphering data (in the present embodiment, the common key encrypting system is employed, and accordingly, the deciphering data is identical to the ciphering data which is used either the ciphering and deciphering). It should be noted that the ciphering data (deciphering data) is stored (added) to the deciphering data

table 204a in relationship with the PC 221 as the ciphering data exchanging protocol is executed.

[0091] The printing unit 205, the display unit 206 and the operation unit 207 are the same as the printing unit 105, the display unit 106 and the operation unit 107, respectively, and accordingly the description thereof will not be repeated.

[0092] The RF module 208 is a module used for the wireless communication. Typically, the RF module 208 is a digital circuit including a transmitter and a receiver. The RF module 208 is connected to the system bus 210 through a not shown I/O interface. The RF module 208 is connected with the directional antenna 211 and the omnidirectional antenna 212 through the antenna switching unit 209.

[0093] It is preferable that the directional antenna 211 and the omnidirectional antenna 212 are configured to transmit/receive the radio wave of the same frequency band, and to use the common circuit (i.e., RF module 208).

[0094] The antenna switching unit 209 is for switching the antenna to be connected with the RF module 208, and is connected with the directional antenna 211 and the omnidirectional antenna 212. The antenna switching unit 209 switches the antenna connected with the RF module 208 between the directional antenna 211 and the omnidirectional antenna 212 based on the program for receiving the encrypted data from the terminal device, under control of the CPU 202.

[0095] The directional antenna 211 is capable of transmitting/receiving radio wave to/from a specific direction (i.e., the directional antenna 211 is designed to perform a directional wireless communication). As examples of the directional antenna, the Yagi antenna and the parabolic antenna have been well known.

[0096] The omnidirectional antenna 212 transmits a radio wave in non-specified direction (i.e., the omnidirectional antenna 212 is not designed for a directional wireless communication). As described above, the omnidirectional antenna 212 is connected with the RF module 208. As examples of the omnidirectional antenna 212, the diversity antenna and the whip antenna are well known.

[0097] The timer 213 has a function of measuring time, and is connected to the system bus 210 through a not shown I/O interface. Using the timer 213, the CPU 202 controls the antenna switching unit 209 to switch the antenna to be connected with the RF module 208 between the directional antenna 211 and the omnidirectional antenna 212.

[0098] As shown in Fig. 6, the PC 221 includes a CPU 222, a ROM 223, a RAM 224, an HDD (Hard Disk Driver) 225, a display unit 226, an operation unit 227, an RF module 228 and an omnidirectional antenna 233. The CPU 222, the ROM 223, the RAM 224, the HDD 225, the display unit 226, the operation unit 227, the RF module 228 are interconnected through a system bus 230.

The omnidirectional antenna 232 is connected to the RF module 228.

[0099] The CPU 222 controls the entire operation of the PC 221. The CPU 222 is selectively retrieves programs (e.g., an encrypting program 225a) from the HDD 225, for encrypting the data to be transmitted, and transmits the encrypted data to an electronic device (e.g., the printer 201) as print data.

[0100] The ROM 223 and the RAM 224 are similar to the ROM 123 and the RAM 124 of the first embodiment, respectively, and the description thereof will be omitted.

[0101] The RF module 228 is a module used for the wireless communication. Typically, the RF module 228 is a digital circuit including a transmitter and a receiver. The RF module 128 is connected to the system bus 130 through a not shown I/O interface. The RF module 128 is connected with the directional antenna 131 and the omnidirectional antenna 132 through the antenna switching unit 129.

[0102] The HDD 225 includes a readable/writable medium (i.e., a hard disk) and a device for reading/writing data from/on the hard disk. In the HDD 225, the encrypting program 225a, a ciphering data table 225b, and the data to be transmitted to the printer 201 are stored.

[0103] The encrypting program 225a encrypts data using the ciphering data stored in the ciphering data table 225b. It should be noted that the ciphering data table 225b is for storing

the ciphering data, which is transmitted from the printer 201. According to the embodiment, the common key encrypting system is employed, and therefore the same key is used for encrypting and decoding. That is, the ciphering data is identical to the deciphering data.

[0104] The RF module 228 is used for executing the wireless communication. The RF module 228 is a digital circuit including a transmitting device and a receiving device. The RF module 228 is connected with the system bus 230 through an I/O interface (not shown). The RF module 228 is connected to the omnidirectional antenna 233.

[0105] The omnidirectional antenna 233 transmits a radio wave in non-specified direction (i.e., the omnidirectional antenna 233 is not designed for a directional wireless communication). As examples of the omnidirectional antenna 233, a diversity antenna and a whip antenna are well known.

[0106] Next, an electronic device 11 (e.g., the printer 201) and a terminal device 12 (e.g., the PC 221) according to the second embodiment will be described in detail.

[0107] Fig. 7 schematically shows an appearance of the electronic device 11 (e.g., the printer 201 of Fig. 6), and Fig. 8 schematically shows an appearance of the terminal device 12 (e.g., the PC 221 of Fig. 6). It should be noted that, the electronic device 11 needs not be limited to the printer 201, and any other apparatus and equipment, which stores, prints

and/or transmits image data and/or document data having secrecy, such as a multifunction peripheral having functions of a facsimile device and the printer, a facsimile machine, a scanner, a device having functions of a file server or a file storage, a stream server, a wireless LAN access point, a Bluetooth access point, may be used as the electronic device 11.

[0108] The electronic device 11 is provided with a directional antenna 11a (e.g., the directional antenna 211 of Fig. 6) and an omnidirectional antenna 11b (e.g., the omnidirectional antenna 212 shown in Fig. 6). As the directional antenna 11a, the Yagi antenna or the parabolic antenna can be used. As the omnidirectional antenna 11b, a diversity antenna or a whip antenna can be used. The directional antenna 11a may be formed integrally with the body of the electronic device 11. Alternatively, the directional antenna may be of a card having a built-in antenna. Similarly, the omnidirectional antenna 11b may be formed integrally with the body of the electronic device 11 or a card type device having a built-in antenna.

[0109] A table 11d is provided to the body of the electronic device 11 so as to be opened/closed. When the table 11d is opened as show in Fig. 7, the terminal device 12 can be placed thereon. Preferably, when the terminal device 12 is placed on the table 11d, a transmission direction of the directional antenna 11a and a receiving direction of an omnidirectional antenna 12c (e.g., the omnidirectional antenna 233) meet each other. It

should be noted that the table 11d needs not be provided to the electronic device 11.

[0110] The terminal device 12 needs not be limited to the PC 221, and any other apparatus, that makes use of other electronic device for obtaining, storing, printing and/or transmitting image data and/or document data having secrecy, such as a PDA (Personal Digital Assistant), a cellular phone, a portable game machine, a wireless digital camera, and a wireless video camera can be used as the terminal device 12. The terminal device 12 is provided with an omnidirectional antenna 12c. As the omnidirectional antenna 12c, the diversity antenna and the whip antenna can be used. It should be noted that the omnidirectional antenna 12c may be a card type device having the built-in antenna as shown in Fig. 8 or one integrally formed to the body of the terminal device 12.

[0111] Next, a procedure, executed in the electronic device 11, for receiving the encrypted data from the terminal device 12 will be described with reference to Figs. 9 and 10.

[0112] Fig. 9 is a flowchart illustrating a receiving procedure executed by a CPU of the printer 201, and Fig. 10 is a flowchart illustrating a normal data communication called in the receiving procedure shown in Fig. 9.

[0113] As shown in Fig. 9, the CPU 202 of the printer 201 (i.e., the electronic device) controls the antenna switching unit 209 to turn ON the omnidirectional antenna 212, and turn

OFF the directional antenna 211 (S201).

[0114] In S202, the CPU 202 controls the timer 213 for measuring a predetermined interval. It is preferable that the predetermined interval is set, in advance, by the user.

[0115] When the predetermined interval has not elapsed (S203: NO), the normal data communication is executed in S209. When the predetermined interval has elapsed (S203: YES), control proceeds to S204, and transmission of the encrypted data is executed.

[0116] In S204, the CPU 202 controls the antenna switching unit 209 to turn OFF the omnidirectional antenna 212, and turn ON the directional antenna 211.

[0117] Then, the CPU 202 determines whether the data is received from the PC 221 in S205.

[0118] When the data has not been received from the PC 221 (S205: NO), control returns to S201. When the data has been received (S205: YES), the CPU 202 determines whether the received data is the encrypted data (S206).

[0119] When the data received from the PC 221 is the encrypted data (S206: YES), the ciphering data has been exchanged, and therefore control returns to S201.

[0120] When the data received from the PC 221 is not the encrypted data (S206: NO), it is necessary to exchange the ciphering data. In this case, the exchanging protocol of the ciphering data for the common key encrypting system is executed

between the directional antenna 211 of the printer 201 and the omnidirectional antenna 233 of the PC 221 to exchange the ciphering data (S207).

[0121] The CPU 202 then registers the ciphering data, which was generated when the exchanging protocol is executed and was transmitted to the PC 221, with the ciphering data table (i.e., the deciphering data table 204a stored in the RAM 204) in relationship with the PC 221 (S208). Thereafter, control returns to S201. It should be noted that, in the PC 221, similarly to the above, the ciphering data received from the PC 221 is registered with the ciphering data table 225a in relationship with the printer 201.

[0122] Next, the normal data communication will be described with reference to Fig. 10.

[0123] Firstly, in this procedure, the CPU 202 determines whether data is received from the PC 221 (S20901). When no data is received (S20901: NO), the normal data communication procedure is finished. When the data has been received (S20901: YES), the CPU 202 determines whether the data transmitted from the omnidirectional antenna 233 of the PC 221 and received by the omnidirectional antenna 212 of the printer 201 is the encrypted data (S20902).

[0124] When the received data is not the encrypted data (S20902: NO), the normal data communication procedure is finished. When the received data is the encrypted data (S20902:

YES), the CPU 202 further determines whether the ciphering data is stored in the deciphering data table 204a in relationship with the PC 221 and the encrypted data can be decoded using the stored ciphering data (S20903).

[0125] When the CPU 202 determines that the encrypted data cannot be decoded (S20903: NO), the normal data communication procedure is finished. When the CPU 202 determines that the encrypted data can be decoded (S20903: YES), the CPU 202 executes the deciphering program 203a to decode the encrypted data using the ciphering data, which is stored in the deciphering data table 204a in relationship with the PC 221, and prints out the decoded data with the printing unit 205 (S20904). Then, the normal data communication procedure is finished.

[0126] It should be noted that, in the PC 221, the encrypted data is encrypted by the ciphering program 225a using the ciphering data which is exchanged and registered with the ciphering data table 225a in S207.

[0127] It should be noted that the communication between the omnidirectional antenna 233 and the directional antenna 211, and the communication between the omnidirectional antenna 233 and the omnidirectional antenna 212 are executed using the same communication protocol. When the same communication protocol is used, only communication paths are different, and the wireless signal processing operations are identical. Therefore,

the processing of the wireless signals becomes identical, which is convenient.

[0128] As above, with the communication system according to the second embodiment, the ciphering data to be referred to for deciphering, which is stored in the deciphering data table 204a of the printer 201 is transmitted through the directional antenna 211 (S204-S207).

[0129] As a result, the PC 221 which can receive the ciphering data is limited, and a possibility of the tapping of the ciphering data is lowered, and accordingly, the secrecy of the secret data can be improved.

[0130] Further, according to the second embodiment, the encrypted data using the ciphering data is transmitted from the PC 221 using the omnidirectional antenna 212 (S201 and S209). As a result, the printer 201 can receive the encrypted data transmitted from the PC 221 along various directions, which is convenient.

[0131] As described above, a directional mode transmission of the wireless signal can be realized using a generally used directional antenna 212 (e.g., the Yagi antenna), and the omnidirectional mode transmission of the wireless signal is realized using the generally used omnidirectional antenna 211 (e.g., the diversity antenna).

[0132] According to the communication system described above, only by configuring the printer 201 to perform the

directional mode transmission of the wireless signal and the omnidirectional mode transmission of the wireless signal, the secrecy is improved. No extra structures of improving the secrecy need not be provided to the PC 221 or the printer 201 are required. Thus, the secrecy of the entire system can be improved relatively simply.

[0133] It should be noted that the present invention needs not be limited to the configurations of the above-described exemplary embodiments, and various modification can be made without departing from the scope of the invention.

[0134] In the above-described first embodiment, in order to achieve the directional mode transmission of the signal and the omnidirectional mode transmission of the signal, the PC 121 is provided with the directional antenna 131 and the omnidirectional antenna 132, and the antenna switching unit 129 is controlled to selectively use them. The invention needs not be limited to such a configuration. For example, the PC 121 may be provided with a single antenna that can be deformed to function as either the directional antenna or the omnidirectional antenna. Similarly, in the second embodiment, the printer 201 may be provided with a single antenna which can function as either the directional antenna 211 or the omnidirectional antenna 212.

[0135] In the first and second embodiments described above, the common key encrypting system using the same key as the

ciphering and deciphering key is employed. The invention can be applied to the communication system employing the encrypting system using the ciphering and deciphering keys that are different from each other. In such a case, the deciphering key is transmitted through the directional antenna. Although the ciphering data (deciphering data) is transmitted in the above-described embodiments, information for identifying key data (i.e., deciphering data) used to decode the encrypted data may be transmitted instead of the key data itself.

[0136] In the above described embodiments, an electromagnetic wave is used for the wireless transmission. As a protocol of the wireless transmission, one according to a wireless LAN (e.g., IEEE 802.11a, IEEE 802.11b and IEEE 802.11g) or one according to the Bluetooth® technology can be employed. When the protocols according to IEEE 802.11a, IEEE 802.11b, and IEEE 802.11g are employed, transmission distance ranges will be 20-90 m, 50-180 m, and 20-180 m, respectively. When the Bluetooth® technology is used, the transmission distance range is 10-100m. Therefore, it becomes unnecessary to arrange the terminal device and the electronic device close to each other.

[0137] The present disclosure relates to the subject matter contained in Japanese Patent Application No. 2002-33104, filed on November 18, 2002, which is expressly incorporated herein by reference in its entirety.